IT Security Requirements for the Processing, Storage and Transmittal of Protected B Information

Contract #:	As per standing offer and related call up number
Department:	AAFC-AAC
Contractor/Supplier:	As per Standing Offer

1. INTRODUCTION

This document outlines the Department's IT Security requirements, in conjunction with any other Canadian Industrial Security Directorate (CISD) requirements, in support of the Contractor/Supplier obtaining an official CISD written approval to use their IT system to process and store Protected B information.

In absence of a formal Threat-Risk Assessment (TRA) and due to the IT portion of the Security clearance being contract specific, the intent of this document is to state the minimum safeguards required in order that the processing and storage of Protected B information be approved by the Department's IT Security Coordinator (ITSC).

Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITS) to effectively safeguard the information, they must be preceded and supported by other aspects of security and the associated policies. The physical, personnel and information security safeguards in accordance with the Policy on Government Security and ITS related Standards must exist prior to the implementation of ITS safeguards.

2. MANDATORY PREREQUISITES

2.1. PWGSC Validation for Physical Security

The application of the security safeguards listed in this document are based on the *mandatory requirement* that the physical premises of the Contractor/Supplier have been inspected, certified and accredited to process and store Protected B information by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services. Hence, for the duration of this contract, the Contractor/Supplier must hold a valid Designated Organization Screening (DOS) with approved Document Safeguarding at the level of Protected B issued by the CISD.

2.2. Personnel Security

All Contractor/Supplier personnel who have access to the material being processed and stored must hold a valid Government of Canada (GC) Reliability Check and Status or a Security Clearance and have the "*need to know*".

All of the Contractor/Supplier personnel handling Protected B information, in relation to this contract, must attend a mandatory security training/briefing session coordinated and delivered by the Contractor's/Supplier's appointed Company Security Officer or alternates.

2.3. Information Security

All hard copy documents and other media formats must be handled and transported in accordance with GC guidelines. All hard copy documents and other media will be marked with the appropriate security classification. Any covering letter, transmittal form or circulation slip will be marked to indicate the highest level of classification of the attachments.

Transportation of information associated with this contract into or out of the physical premises must adhere to RCMP G1-009 "*Transport and Transmittal of Protected and Classified Information*". All processing and storage of Protected B information must be performed within the confines of CISD approved physical locations for this contract.

2.4. Security Policy Compliance Monitoring

The Department retains the right to conduct inspections of the Contractor/Supplier facility to ensure compliance with GC standards and policies with respect to the handling, storage and processing of information relevant to this contract.

3. MINIMUM IT SECURITY REQUIREMENTS

In conjunction with any other requirements established by the CISD, the Contractor/Supplier must meet the following IT Security requirements established by the Department.

Furthermore, the Contractor/Supplier must ensure that effective security controls are in place to protect medium level Confidentiality and Integrity and, at minimum, medium level Availability. Communications Security Establishment Canada's (CSEC's) recommendations and guidelines must be followed. Their published ITSG-33 documentation will provide further details.

3.1. IT Security Policy Compliance and Monitoring

All information technology related operations must adhere to the overall requirements outlined in the GC's Operational Security Standard: Management of Information Technology Security (MITS). All IT Security requirements addressed to the Department are applicable to the Contractor/Supplier.

The Department retains the right to conduct inspections of the Contractor/Supplier facility to ensure compliance with GC policies and standards with respect to requirements in the Operational Security Standard: Management of Information Technology Security.

3.2. Prevention

As per MITS section 16, the Contractor/Supplier must have all the prevention safeguards in place for the protection of confidentiality, integrity, and availability of the information and IT assets relative to this contract.

3.2.1 Physical Security within the IT Security Environment

Along with providing official assurance that the CISD has approved its facilities to process and store Protected B information, the Contractor/Supplier must ensure that all equipment used for the fulfilment of this contract reside within the CISD approved physical locations.

The Contractor/Supplier must protect all equipment being used for this contract. The use of wireless technology must be approved by the Communications Security Establishment of Canada (CSEC) for the information's level of sensitivity and follow guidance in CSEC's ITSPSR-21A.

3.2.2 Storage, Disposal and Destruction of IT Media

All material such as CD/DVDs, flash/thumb drives, workstation hard disks, server hard disks, backup tapes and any other devices used to process or store Protected B information relative to this contract must be identified and labelled accordingly.

In the event of failure and replacement of the equipment or upon termination of the contract, all devices or material must be retained and properly stored or disposed of according to CSEC recommendations. The Contactor/Supplier is also responsible for clearing and sanitizing all electronic data storage devices used for this contract according to CSEC's ITSG-06 guideline.

In the event that equipment requires maintenance, support or replacement, no hardware associated with the processing or storage of protected information may be given to an outside vendor unless it has been cleared or sanitized according to CSEC recommendations found in the ITSG-06 guideline.

All media, when not in use, must be stored in a storage container which is RCMP-approved for the storage of Protected B information (G1-001 "*Security Equipment Guide*"). The storage container must be verified by the CISD.

3.2.3 Authorization and Access Control

The Contractor/Supplier must restrict IT and information access relative to this contract only to its individuals who have been screened and authorized, have been identified and authenticated, and have a "need to know".

In following the 'principle of least-privilege', the Contractor/Supplier must provide only the minimum access required for individuals to perform their duties.

The Contractor/Supplier must withdraw all access privileges relative to this contract from individuals no longer involved.

3.2.4 Cryptography, Network Security and Perimeter Defence

The electronic storage of Protected B information associated with this contract must be within a CISD approved IT environment.

Electronic transmission of Protected B information must be encrypted using CSEC approved technology such as Entrust Security Provider and the GC Public Key Infrastructure.

The Contractor/Supplier must segregate its networks into IT security zones and implement perimeter defence and network security safeguards. CSEC provides the ITSG-38 and ITSG-22 guidelines on this specific subject. As well, the Contractor/Supplier must apply strict control of all access to the protected zone where the information associated with this contract resides. Network perimeter defence safeguards (e.g. firewalls, routers) must be used to mediate all traffic and to protect servers that are accessible from the internet. The Contractor/Supplier must use CSEC approved encryption technology to ensure confidentiality, integrity, authentication and non-repudiation.

The Need-to-Know principle must be applied and transmission must be restricted only to CISD approved recipients.

3.2.5 Mobile Computing and Teleworking

All processing and storage of Protected B information must be performed within the confines of the CISD approved physical locations for this contract.

3.2.6 Software Integrity and Security Configuration

The Contractor/Supplier should configure the security of their operating systems and application software being used to process Protected B information in accordance with security best practices (such as the Microsoft Security Compliance Toolkits for servers and clients). Safeguards must be implemented to "harden" servers and workstations processing Protected B information. For more information on software hardening and configuration best practices, refer to the best practices issued by CSEC, by the National Institute for Standards and Technology (NIST) and by the Center for Internet Security.

3.2.7 Malicious Code

The Contractor/Supplier must install, use and regularly update antivirus software and conduct scans on all electronic files from external systems.

3.3. Detection

It is important to have the ability to detect security related issues within the operating environment. The rigor and extent of detection must be based on a medium level of risk. To protect the information associated with this contract and ensure service delivery, the Contractor/Supplier must continuously monitor system performance to rapidly detect:

- Attempts (failed or successful) to gain unauthorized access to a system, or to bypass security mechanisms.
- Unauthorized probes or scans to identify system vulnerabilities.
- Unplanned disruption of systems or services.
- Denial-of-service attacks
- Unauthorized changes to system hardware, firmware, or software.
- System performance anomalies, and
- Known attack signatures.

At minimum, the Contractor/Supplier must include a security audit log function in all IT systems.

3.4. Response and Recovery

3.4.1 Incident Response

The Contractor/Supplier must establish mechanisms to respond effectively to IT incidents and exchange incident-related information with the Department immediately. The Contractor/Supplier must have a documented incident response process.

3.4.2 Incident Reporting

It is paramount that the Department is made aware of any security-related incidents with respect to the facilities and equipment used to process and store Protected B information associated with this contract.

The Contractor/Supplier must report any security-related incidents to the Department within *two hours* of an incident being detected or reported.

3.4.3 Recovery

Before reconnecting or restoring services, the Contractor/Supplier must ensure that all malicious software has been removed and that there is no potential for recurrence or spread.

With regards to the information associated with this contract, the Contractor/Supplier must:

- Back up the data regularly
- Test backups regularly to ensure that they can be used for recovery
- Back up all software and configuration data

- Facilitate the restoration of data and services by allowing systems to undo operations and return to an earlier state.
- Test restoration procedures regularly to ensure that they are effective and that they can be completed within the time allotted for recovery.
- Determine retention periods for essential business information and archived backups, and
- Ensure that off-site backup storage is within a CISD approved location if no CSEC approved encryption is being used.

Note that system recovery should be conducted in a manner that preserves the integrity of evidence, in the event of a criminal investigation of a security breach, for example.

4. CONCLUSION

In absence of a formal TRA, this document has established the Department's basic IT Security requirements for the processing and storage of up to and including Protected B information.

Through the Canadian Industrial Security Directorate's invaluable input and expertise at certifying that the Contractor/Supplier has met all IT Security requirements, the Department will be reassured that risks have, most likely, been mitigated to acceptable levels.